

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH FACEBOOK  
 USER ID "BæBae Løw,  
 http://www.facebook.com/profile.php?  
 id=100039661731437"

)  
)  
)  
)  
)  
)  
)

Case No. 20 MJ-101

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Please see Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

Please see Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1503 and 1512(b)(1)

The application is based on these facts: See attached affidavit.

☒ Delayed notice of <sup>30</sup> days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Mason Kohlapp #247  
 Applicant's signature

Mason Kohlapp, FBI TFO  
 Printed Name and Title

Sworn to before me and signed in my presence:

Date: 3/5/2020

William E. Dyff  
 Judge's signature

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
FACEBOOK USER ID "BæBæ Low,  
<http://www.facebook.com/profile.php?id=100039661731437> THAT IS STORED AT  
PREMISES CONTROLLED BY  
FACEBOOK INC.

Case No. 20-MJ-101

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Mason J. Kohlhapp, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a federally deputized Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI). I have been a FBI TFO with the Southeastern Wisconsin Regional Gang Task Force (SWRGTF) since March of 2019. During my (4) four years as a Deputy for the Milwaukee County Sheriff's Office, I have received training in the investigation of drug trafficking. I have participated in search warrants, investigations, and arrests in which controlled substances and drug paraphernalia were seized. I am also familiar with social media platforms,

including Facebook, and the various ways criminals use them to further their illegal operations. In my training and experience, I also know that family and friends of individuals charged with crimes will frequently attempt to dissuade the witnesses against them from testifying.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1503 (obstruction of justice) and 1512(b)(1) (witness tampering) have been, are being, and will be committed by Victor L. GONZALEZ, Jr. (DOB: 4/9/2001). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

### **FACEBOOK FUNCTIONALITY**

5. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

6. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

7. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays.

8. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

9. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user

and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

10. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

11. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

12. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

13. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

14. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

15. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

16. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

17. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

18. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

19. Facebook further maintains a functionality it refers to as "Stories," whereby users can post photos and videos using Facebook's "in app" camera, frequently utilizing filters and additional text. After a user "posts" a "Story," the "Story" will be available to their "friends" for a 24-hour period, appearing at the top of their "News Feed" in the application.

20. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

21. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic

context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

22. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

#### **PROBABLE CAUSE**

23. In February of 2019, case agents initiated an investigation into a group of known and unknown drug traffickers operating in the Milwaukee area, known as the Buffum Meinecke Boys (“BMB”), including Ramone LOCKE, aka “Mone,” Amir LOCKE, aka “Big Mir,” Joey VAZQUEZ, aka “Joey,” Louis BATES, aka “Little Louis,” Michael SMITH, aka “M&M,” Garrell HUGHES, aka “Rello,” Jesus PUENTES, aka “JP,” Coury AGEE, aka “Lil C,” Lamar JOHNSON, aka “Fresh,” Luis Lorenzo, aka “Pito,” Victor GONZALEZ, aka “Bey Bey,” and others. As part of the investigation, case agents have interviewed several confidential sources,

conducted physical and electronic surveillance, utilized pen registers, reviewed historical phone toll records, subpoenaed and reviewed records, and conducted controlled purchases of cocaine, crack cocaine, and heroin. As a result of the intelligence provided by the confidential sources and the controlled purchases, along with information obtained from other law enforcement techniques, case agents have identified various members of the BMB and identified several sources of supply.

24. Victor GONZALEZ, aka “Bey Bey,” was indicted on February 18, 2020, in Case No. 20 CR 041, along with many other BMB members, for offenses related to both firearms and controlled substances.

25. On February 25, 2020, state, local and federal officers executed a joint “takedown” of the BMB and related defendants, attempting to simultaneously arrest the charged defendants and search associated locations. Victor GONZALEZ, aka “Bey Bey,” was arrested on that date.

26. Victor L. GONZALEZ, Jr. (DOB: 4/9/2001) is the son of Victor GONZALEZ, aka “Bey Bey.”

27. Law enforcement knows that Victor L. GONZALEZ, Jr. (DOB: 4/9/2001) maintains the Facebook account associated with the Facebook user ID of “**BæBæ Low**,” <http://www.facebook.com/profile.php?id=100039661731437>, based on both (i) its review of postings and other identifiers associated with that same account; and (ii) information provided to law enforcement by a confidential informant hereinafter referred to as CS #3. CS #3 personally knows Victor L. GONZALEZ, Jr. (DOB: 4/9/2001), they have multiple common acquaintances, and CS #3 is familiar with his Facebook profile.

28. Over the last seven days, Victor L. GONZALEZ, Jr.'s Facebook account (as noted above, the he Facebook account associated with the Facebook user ID of "**BæBæ Low**," <http://www.facebook.com/profile.php?id=100039661731437>) posted a "Story" with the following message: "[A common nickname for CS #3 among his friends on Milwaukee's Northeast side] police asab with his rat ass."

29. Based on my experience and training, I know "asab" is vernacular meaning "as a bitch."

30. CS #3 no longer maintains social media profiles, but CS #3 was made aware of this "Story" by one of his mutual acquaintances with Victor L. GONZALEZ, Jr. (DOB: 4/9/2001).

31. Given their many mutual acquaintances and the public nature of Facebook "Stories," I believe that Victor L. GONZALEZ, Jr. (DOB: 4/9/2001) posted the "Story" mentioned above, identifying CS #3 as a cooperator, in an effort to intimidate him/her and dissuade him/her from testifying against Victor GONZALEZ, aka "Bey Bey," and other members of the BMB.

32. I believe that the "Story" mentioned above is still within Facebook's custody and control, as (i) I know Facebook has the capability to, and frequently does, "archive" material of this sort; and (ii) FBI TFO Eric Maldonado has sent a preservation request to Facebook with respect to the account at issue here.

33. I understand that the government has not yet made discovery available in Case No. 20 CR 041, as it intends to seek a protective order. Law enforcement does not yet know how CS #3 was identified as a cooperator by Victor L. GONZALEZ, Jr. (DOB: 4/9/2001).

34. For several reasons, case agents believe CS #3 to be credible and reliable. First, CS #3 has been providing continuous information since September of 2019. Second, the information provided by CS #3 is consistent with evidence obtained elsewhere in this investigation where CS #3 was not utilized, and substantial portions of CS #3's information has been corroborated through independent investigation, including surveillance and information from other sources. CS #3 is cooperating for monetary compensation and has prior felony convictions for armed robbery, heroin trafficking and marijuana trafficking. CS #3 is currently on state supervised release. For these reasons, case agents believe CS #3 to be reliable.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

#### **CONCLUSION**

36. Based on the foregoing, I request that the Court issue the proposed search warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Facebook. Because the warrant will be served on Facebook, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

38. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **REQUEST FOR SEALING**

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation and a threat to a confidential informant. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Facebook user ID “**BæBae Low**, **<http://www.facebook.com/profile.php?id=100039661731437>** that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. (“Facebook”), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from February 25, 2020, to the present;
- (c) All “Stories” posted by the account from February 25, 2020, to the present;
- (d) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from February 25, 2020, to the present, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (e) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (f) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (g) All other records and contents of communications and messages made or received by the account from February 25, 2020, to the present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (h) All "check ins" and other location information;
- (i) All IP logs, including all records of the IP addresses that logged into the account;
- (j) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (k) All information about the Facebook pages that the account is or was a "fan" of;
- (l) All past and present lists of friends created by the account;
- (m) All records of Facebook searches performed by the account from February 25, 2020, to the present;
- (n) All information about the user's access and use of Facebook Marketplace;
- (o) The types of service utilized by the user;

- (p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (q) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (r) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within ten days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1503 and 1512(b)(1) involving Victor L. GONZALEZ, Jr. (DOB: 4/9/2001) since February 25, 2020, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Either the identification of, or threats to, witnesses involved in ongoing criminal investigations;
- (b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- (c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.